State of Michigan

Biennial Evaluation of the
Internal Control Structure (ICS)
in Effect During the Two-year Period Ended September 30, 2000

The Management and Budget Act (Sections 18.1483 – 18.489 of the Michigan Compiled Laws) requires a biennial evaluation of each department's internal control structure [1]. Results of these evaluations, including a description of any material weaknesses identified, and plans and time schedules for correcting them, must be reported by the department director to the Governor, Auditor General, Legislature, and the Department of Management and Budget (DMB). The current biennial cycle ends September 30, 2000 with the reports due by May 1, 2001. Examples of sample reports are included in *Administrative Guide to State Government* (procedure 1270.01).

The DMB, Office of Financial Management (OFM) recently (December 1999) issued guidance for conducting evaluations of departmental internal controls. This guidance, formally titled *Evaluation of Internal Controls: A General Framework and System of Reporting,* represents a comprehensive revision to the guidance last issued in 1990. The new guidance incorporates concepts set forth in a widely accepted internal control framework entitled "*Internal Control - Integrated Framework*" - prepared by the "COSO" (Committee of Sponsoring Organizations of the Treadway Commission- the federally sponsored group responsible for development of the framework).

This document contains instructions to departments for using the referenced evaluation worksheets in conducting evaluations of their respective internal control structure. Throughout these instructions, the worksheets are electronically linked to other locations on the OFM web site. The worksheets were constructed using concepts presented in the general framework guidance. Departments should use these tools, or alternative evaluation tools, to evaluate and document their internal control structure. Use of the referenced tool sets should result in a substantive, effective evaluation of your department's internal control structure. See the section "Reference to Evaluation Tools" in DMB's general framework for considerations when selecting / using appropriate evaluation tools.

The worksheets referred to in these instructions address each component of internal control: Control Environment, Risk Assessment, Control Activities, Information & Communication, and Monitoring.

The following worksheets are included:

- Evaluating the Control Environment Component of the ICS
- Evaluating the Information and Communication Component of the ICS
- Evaluating the Risks, Control Activities, and Monitoring Components of the ICS (for non-financial activities)
- Evaluating the Risks, Control Activities, and Monitoring Components of the ICS Associated with Financial Management Activities
- Evaluating Automated Information Systems / Data Center Controls

The new guidance for evaluating internal controls focuses attention on departmental "activities" that contribute towards achievement of their missions and underlying objectives. An "activity" may be defined as one or several organizational components that seek to achieve common business objectives. Alternatively, the activity may correlate with a core business process that "cuts across"

multiple activities (i.e., support functions including administrative activities, human resources, and information technology).

Management responsible for achievement of objectives in each of the department's identified activities should complete their evaluations in accordance with the guidelines issued by DMB – OFM. Departmental evaluations are **not** intended to assess opportunities for operational improvements such as staff additions, automation enhancements or other resource increases. Those are considered annually as part of the executive budget process and are not to be included in the biennial evaluation process. If material weaknesses (as defined in the internal control guidance issued by DMB) are identified that require additional resources to control, the department should prepare corrective action plans redirecting existing resources, including substantive evidence and quantifiable operational impact statements resulting from resource reallocation.

These new tools highlight the importance of "soft" control activities; this differs from traditional internal control assessment tools, such as those provided by DMB for prior evaluations. "Soft" controls are intangibles that management emphasizes to direct the organization, which includes integrity, ethical values, communication, philosophy, operating style, organizational commitment to competence, and the understanding and management of risk.

Evaluation worksheets are in a narrative format requiring written responses. Generally, responses will not be "yes" or "no," but rather information on how "activity managers" address each item included on the worksheets. The evaluator should provide detailed information about management's internal control structure and provide documentation to support their conclusions.

Departmental management responsible for *financial management activities* should complete the evaluation of internal control structure over accounting activities and financial practices. The approach for evaluating internal controls over *non-financial activities* is identical to that used for evaluating internal controls over financial activities – however, *the activity level objectives* will differ. Evaluators of each departmental activity should use the worksheets to identify, document, and evaluate the risks and controls related to achievement of the objectives it seeks to attain.

A worksheet is also included for documenting controls over activities for developing, maintaining, and operating *automated information systems*. Departments should consider formation of a multi-disciplinary team to evaluate controls over these information systems because many of the risks and control activities are the responsibility of the department's Information Technology organization, non-IT activities (i.e., program managers which function as the "application owners"), or both. *The COBIT - Control Objectives* document is included as reference material for use in evaluating internal controls in automated information systems. It includes a detailed listing of control objectives for each of the primary "processes" (i.e., activities) typically in place to support development, maintenance, and operation of information and related technology.

Space is provided at the end of each worksheet for appropriate agency personnel to **"Certify"** his/her overall evaluation conclusions. The person responsible for the conclusions should sign the certification, either the DSO, in the case of a department-wide evaluation, or the activity level manager, for activity level evaluations. Certification attests to the sufficiency or effectiveness of the respective activity's internal control structure. Departments should submit a description of corrective action plans and time frames for addressing material weaknesses identified in connection with this biennial evaluation.

Departments may use either hardcopy or electronic worksheets to document evaluation responses and conclusions. Electronic worksheets are available for download (MS Word 95/v 6.0) via OFM's web site and can be customized to allow for additional space for documenting the evaluation and associated conclusions. Attach additional narratives/explanations to the worksheets to further document how items apply to the department. If applicable formal (written) policies or procedures are mentioned, identify/reference such policies. If informal policies,

procedures or practices are mentioned as representing controls, document these and provide copies along with the completed evaluation worksheets.

[1] The Management and Budget Act uses the term Internal Accounting and Administrative Control System. This term can be used interchangeably with Internal Control, Internal Control Structure, or System of Internal Control - all are comparable.

Worksheet Instructions for:
Evaluating the Control Environment Component of the ICS
and
Evaluating the Information and Communication Component of the ICS

These worksheets focus on common factors (objectives and risks) relevant to the Control Environment and Information and Communication components of the department's overall internal control structure. These worksheets should be used to conduct evaluations of components at the department-wide perspective and, where applicable, at the activity level. For example, activity level management may not be concerned with the objective that all departmental objectives are consistent and interrelated. However, activity level managers should be knowledgeable about the effectiveness of all internal control components and must evaluate elements of the internal control component for which they are responsible.

General Instructions and Considerations
Respond to each item from the perspective of the activity manager completing the evaluation. If this is not practical, address the item from the perspective of, or with regard to the department as a whole. Focus your responses on policies, practices or procedures of the individual activity or identify departmental policies, procedures or practices that impact/apply to the activity being evaluated. Listed below each item are examples of subsidiary issues to illustrate the types of issues to consider; many other issues will likely be relevant.
Use the second column, "Description/Comments on Policies/Procedures/Practices," to provide comments and a detailed description of the strengths and weaknesses of existing control activities employed to achieve objectives / criteria identified in the first column.
At the end of each section, space is provided to record a conclusion on the effectiveness of related controls and management's proposed actions (i.e., corrective actions) to address identified control weaknesses.

Worksheet Instructions for:
Evaluating the Risks, Control Activities, and Monitoring Components of the ICS (for non-financial activities)

Each activity level manager should use this worksheet to evaluate and document internal controls that contribute towards the achievement of activity level objectives. Results of activity level evaluations should be considered when performing the department's overall evaluation of internal controls that contribute towards the achievement of department-wide objectives, using the approach presented in this worksheet.

General Instructions and Considerations
For purposes of complying with the biennial evaluation requirements, evaluators should focus the evaluation and documentation on **significant** activity level and/or department-wide objectives being evaluated. Significance may be based upon the fiscal size of the activity (i.e.,

budget/expenditures) and the degree of inherent risks in the activity / process (e.g., cash collections, inventory susceptible to theft, confidentiality of information, degree of potential political/legislative or media interest, etc.). Management should evaluate the internal control structure over the non-significant, incidental or non-critical activities/objectives during the course of normal operations – not necessarily to support the biennial evaluation requirements.

Typically, personnel responsible for managing non-financial activities will not be requested to complete separate worksheets for internal controls over financial/accounting practices – this is the responsibility of your department's financial management. When an activity level objective is financial in nature, and much of the control is the responsibility of the department's financial management personnel, the evaluator should indicate the importance of the objective, and note that they are relying on the appropriate personnel responsible for controlling the associated risks. Furthermore, the evaluator should consult with the responsible financial management to gain an understanding of how the (financial management) risks are mitigated, and consider implementing additional control activities by either management of the activity being evaluated or the financial management personnel. Top leadership should be involved in decisions on where (i.e., under what manager's responsibility) controls should be enhanced / added.

Specific Instructions

- *Activity Level Objective (Column 1)* - Identify the significant activity level objectives being evaluated. The worksheet includes space for 6 objectives for illustrative purposes (more or fewer may be evaluated, based upon the evaluator's judgment as to significance). **Examples** of activity level objectives include completing customer projects in a timely manner; ensuring services provided meet quality standards; ensuring work environments/conditions comply with laws, regulations.

- *Risk Factors (Column 2)* **-** Identify risks associated with each significant activity level objective. Risks may be identified as the result of answering the following types of questions: 1) "What is the potential result of not efficiently/effectively performing control activities to meet a specific operating objective?" or 2) "What are potential effects on reliability of financial reporting, compliance with laws and regulations, safeguarding of program assets, efficient use of program resources?"). **Examples** of risks include failure to complete customer projects timely, providing services that do not meet established quality standards, work environment/conditions that violate applicable laws, regulations, etc.

- *Actions / Control Activities (Column 3)* **-** Identify control activities (policies, procedures or practices) that exist within the activity that mitigate identified risks. Be as detailed as possible; describe specific control activities that do not represent formal policies/procedures or are not otherwise documented. **Examples** of control activities include production/project management, customer satisfaction evaluation procedures, cost containment controls (labor and materials), procedures for accumulating administrative and related federal program costs, management/supervisory review of various processes, quality assurance monitoring procedures, etc.

  Generally, identify control activities that:

  - Provide separation of duties and responsibilities among employees.
  - Limit access to State resources to authorized personnel requiring access within scope of assigned duties.
  - Assure appropriate authorizations and record-keeping procedures are used to control assets, liabilities, revenues, and expenditures.

- Assure established policies and procedures are followed in performance of assigned functions.
- Ensure personnel are qualified and maintain a sufficient level of competency.
- Ensure activity level objectives are accomplished efficiently.

- *Monitoring (Column 4)* - Identify monitoring activities used by the activity manager to ensure established internal controls are operating and effectively address identified risks. Include results of testing conducted under the direction of management as evidence to support conclusions. Provide detailed responses; describe specific monitoring activities that do not represent formal policies/procedures or are not otherwise documented.

- *Conclusions (Column 5)* - Record a conclusion on the sufficiency/effectiveness of existing internal controls, and proposed actions (i.e., corrective actions) to address internal control weaknesses. Monitoring activities are the key factor in concluding about the effectiveness of control activities. It is difficult for an activity manager to reach conclusions about the effectiveness of control procedures without first implementing appropriate monitoring activities.

Worksheet Instructions for:
Evaluating the Risks, Control Activities, and Monitoring Components of the ICS Associated with Financial Management Activities

Typically, management responsible for the department's overall financial operations will complete this worksheet. The information resulting from this evaluation should be shared with all personnel in the department (e.g., other activity managers) to strengthen an overall understanding and implementation of controls over financial activities, and to minimize duplication of effort.

Specific Instructions

- *Objectives (Column 1)* - Identifies operational, financial reporting, and compliance objectives related to financial/accounting activities.

- *Control Objective Type (Column 2)* – Indicates the nature of the objective identified in column 1, in relation to the broad objectives achieved through an effective internal control structure. This column is useful in summarizing overall conclusions about the effectiveness of the internal control structure over financial management activities. The broad categories of objectives include:

  "O" - Operational effectiveness and efficiency in the use of departmental resources.
  "F" - Reliable preparation of financial statements and schedules.
  "C" - Compliance with applicable laws, regulations, and management directives.

- *Risk Analysis (Column 3)* - Identifies common risks associated with the objectives; answers questions such as: ("What is the potential result of not having proper controls over financial/accounting transactions?" "What are potential effects on reliability of financial reporting, compliance with laws and regulations, and safeguarding of program assets?"). The risk analysis should consider the significance of the risk (i.e., potential adverse effects) and the likelihood or frequency of its occurrence. This leads logically

into the analysis of how management should manage the risk, which is documented in subsequent column #4.

- *Actions / Control Activities (Column 4)* - Identifies actions/control activities (policies, procedures or practices) in place to minimize risks and contribute towards achievement of the objective identified in column #1. Provide detailed responses; describe specific control practices that do not represent formal policies/procedures or are not otherwise documented by the activity.

  Generally, identify control activities that:

  - Provide separation of duties and responsibilities among employees.
  - Limit access to State resources to authorized personnel requiring access within scope of assigned duties.
  - Assure appropriate authorizations and record-keeping procedures are used to control assets, liabilities, revenues, and expenditures.
  - Assure established policies and procedures are followed in performance of assigned functions.
  - Ensure personnel are qualified and maintain a sufficient level of competency.
  - Ensure program objectives are accomplished efficiently.

- *Monitoring (Column 5)* - Identify monitoring activities in place to ensure established internal controls are operating and effectively address identified risks. Include results of testing conducted under the direction of management as evidence to support conclusions. Provide detailed responses; describe specific monitoring activities that do not represent formal policies/procedures or are not otherwise documented.

- *Conclusions (Column 6)* - Record a conclusion on the sufficiency/effectiveness of existing internal controls, and proposed actions (i.e., corrective actions) to address internal control weaknesses. Monitoring activities are the key factor in concluding about the effectiveness of control activities. It is difficult for management to reach a conclusion about the effectiveness of control procedures without first implementing appropriate monitoring activities.

Worksheet Instructions for:
Evaluating Automated Information Systems / Data Center Controls

General Instructions and Considerations

Due to the increasing dependency on automated systems, a worksheet was developed for documenting controls in the department's automated information systems/data center environments. This evaluation and documentation process is critical for departments responsible for administering critical information systems that support departmental business processes. The worksheet related to these instructions was prepared from a commercial product; ***CobiT: Control Objectives for Information and Related Technology***, developed by Information Systems Audit and Control Foundation (ISACF). This product, for use by IT management/users, and information systems auditors, is considered one of the most effective and widely accepted tools for evaluating security and control in the IT environment.

Information technology (IT) management personnel (e.g., CIO, Director of IT, etc.) is generally **not** responsible for **all** IT processes associated with a particular information system/data center environment. Program managers (i.e., activity level managers) are typically the "application

owners" for which systems are developed and maintained. A collaboration between IT personnel and non-IT activity managers is necessary to evaluate risks / controls over many objectives listed on this worksheet.

You may customize the worksheet during the evaluation process or if using this worksheet for the first time. For example, enter "NA" in worksheet columns for IT processes not the responsibility of the manager completing the worksheet. When appropriate, jointly evaluate controls common to more than one IT environment.

It is critical that you develop documentation of the department's internal control structure/systems, in addition to evaluating the control structure. In past biennial evaluations, documentation efforts have not been sufficiently addressed, particularly for the department's unique IT environments. Improved documentation will reduce efforts/resources required to complete the next biennial evaluation and facilitate periodic monitoring of controls by managers of the information systems/data centers.

Determine if other reviews of information systems and data center operations and/or specific application systems have been conducted recently. When obtaining assurances about the effectiveness of general computer and application controls in the IT environments being evaluated, utilize reviews/audits conducted by the Auditor General, internal evaluations, Statements of Auditing Standards (SAS) 70 reviews, consulting engagements, etc. Attach such documentation, if used in completion of this evaluation worksheet.

Specific Instructions
This worksheet is divided into the following IT categories; each contains up to 13 components/IT processes:

Planning & Organization
Acquisition & Implementation
Delivery & Support
Monitoring

- *Component (Column 1)* – Identifies each component (IT process) at the level that agencies should evaluate and document existing controls in respective IT processes and environments.

- *Risks (Column 2)* - Identifies potential risks that may result from a lack of appropriate policies, procedures and/or controls.

- *Internal Controls (Column 3)* - Summarizes typical elements of a management and control structure that would address risks applicable to each IT process. For each process, a reference is given to detailed control objectives defined by **CobiT - Control Objectives**. Although a separate evaluation of each of the 302 control objectives is not required, due to resource concerns, each should be considered as the worksheet is completed.

  (Use remaining worksheet columns to document assessment of actual internal controls within each IT environment.)

- *Responsible Activity (Column 4)* - Identify the activity (e.g., department/organizational units) responsible for each IT process, particularly when noting specific IT processes in later columns as being not applicable to the responsible activity completing the worksheet.

- *Columns 5-12* – Enter check marks to denote whether appropriate controls (see Column 3) exist within the IT environment being evaluated; and whether controls are documented, effective, and sufficient.

  Existence:
  D - Documented
  ND - Not Documented
  N/A - Not Sure or Not Applicable

  Performance/Effectiveness:
  E - Excellent
  V - Very Good
  S - Satisfactory
  I - Ineffective/Insufficient
  N/A - Not Sure or Not Applicable

- *Description/Comments (Column 13)* - Enter description/comments related to information and conclusions made in previous columns; identify formal policies, procedures, and informal practices that represent internal controls over the IT process and control objectives. Identify, at a minimum, control objectives for which appropriate control activities do not currently exist, whether there are alternative or compensating controls, and whether plans and time frames exist for addressing deficiencies in the control structure.